UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/847,813	05/01/2001	Curt Wohlgemuth	OMNI0008	6351

20995 7590 09/20/2005

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/847,813	WOHLGEMUTH ET AL.	
	Examiner	Art Unit	
	Benjamin E Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 December 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,10-12,19,25 and 31-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,10-12,19,25 and 31-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 1/22/05
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 15 August 2005 amends claims 3, 12, and adds claims 31-44. Applicant's amendment has been fully considered and is entered.

Response to Arguments

2. Applicant's arguments filed 15 August 2005 have been fully considered but they are not persuasive. Applicant's argument that Safadi does not disclose the granting of requests is dependent on information such as: the nature of the originating process, the history of previous access by the process, and/or the section of the targeted file being requested is not persuasive because Safadi discloses that the token can be pre-authorized (Abstract), which meets the limitation of history of previous access because it suggests a previous authorization. Safadi discloses the authorization is performed depending on what is being requested (Col. 2, lines 12-19), which meets the limitation of the section of the targeted file being requested.

3. Applicant's argument Safadi does not disclose the network director component making visible to said network file system, a path that represents the server where said application program files are stored is not persuasive because Safadi when authorized the requesting user is provided access to web sites, or accessing content resident on these sites, or downloading programs from these sites (Col. 4, lines 50-54), which meets the limitation of making a path visible because it is known to those of ordinary skill in the art that when data packets are transmitted across networks, that they are affixed with a source IP address and a destination IP address. Therefore, when received, the IP address of the source is visible in the data packet.

4. Applicant's argument that Safadi does not disclose dispatch routines is not persuasive because the client application of Safadi would meet the limitation of the dispatch routine that examines the file requests and decides whether to grant or deny said file request (Col. 2, lines 1-10, Col. 3, lines 11-17).

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-3, 10-12, 19, 25, 31, 32 are rejected under 35 U.S.C. 102(e) as being anticipated by Safadi, U.S. Patent No. 6,810,525. Referring to claims 1, 10, 19, 25, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of providing a network file system on said client, when said network file system handles and forwards all requests from local processes on said client that are directed at application program files located on said server, wherein said file system examines each of said requests, and either grants or denies each of said requests depending on whether the request is justifiable from a security perspective by using information that includes, but is not limited to: the nature of the originating process, the history of previous access by the process, and/or the section of the targeted file being requested. The client application then sends the entitlement

token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing a network redirector component of said network file system, and wherein said network redirector component makes visible to said network file system, a path that represents the server where said application program files are stored.

Referring to claim 31, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of using a first computer to serve said application program files to a second computer for execution, using a filtering mechanism that is associated with said second computer for filtering requests for access to said application program files, wherein said filtering mechanism determines whether to grant requests for access to said application program files by determining one or more criteria from a set of criteria comprising: a nature of an originating process that is making said requests for access, a history of previous requests for access made by said originating process, and a nature of a section of said application program files that is being requested.

Referring to claim 32, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of providing informaiton relating to one or more remote locations where said application program files are

stored, determining whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy.

Referring to claims 33, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17). The client application of Safadi would meet the limitation of the dispatch routine that examines the file requests and decides whether to grant or deny said file request (Col. 2, lines 1-10, Col. 3, lines 11-17). which meets the limitation of providing information relating to one or more remote locations where said application program files are stored, using dispatch routines for examining a request for access to said application program files, after examining said request and if it is determined that an originating process that is making said request for access is a trusted process, or that a history of previous requests for access made by said originating process lacks a pre-determined pattern of piracy, and that a section of said application program files that is being requested is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said application program files.

Referring to claim 34, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of using a filtering

mechanism on a client computer for filtering requests for access to said application program files, wherein said filtering mechanism determines whether to grant requests for access to said application program files by determining one or more criteria from a set of criteria comprising: a nature of an originating process that is making said requests for access, a history of previous requests for access made by said originating process, and a nature of a section of said application program files that is being requested. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of using a revealing mechanism to reveal to said client computer one or more remote locations on which said requested application program files are stored.

Referring to claim 35, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of a processing device for processing a request for access to said application program files stored on at least one server system that is remote from said processing device, wherein said processing device comprises a component that determines whether to grant requests for access to said application program files based on: whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The client

application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a redirecting component that is associated with said processing device for informing said processing device of one or more locations in which said application program files are stored.

Referring to claim 36, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of processing means for processing a request for access to said application program files stored remotely from said processing means, wherein said processing means includes a determination whether to grant requests for access to said application program files based on: whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a redirection means for revealing one or more locations in which said application program files are stored.

Referring to claim 37, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of a filtering means for filtering requests for access to said application program files stored remotely from said filtering means, wherein said filtering means includes an evaluation means for evaluating: an originating process that is making said requests for access, a history of previous requests for access made by said originating process, and a section of said application program files that is being requested. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a redirection means for revealing one or more locations in which said requested application program files are stored.

Referring to claim 38, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of determining whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's

request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored.

Referring to claim 39, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of using dispatch routines for examining a request for access to said application program files, after examining said request and if it is determined that an originating process that is making said request for access is a trusted process, and that a history of previous requests for access made by said originating process lacks a pre-determined pattern of piracy, and that a section of said application program files that is being requested is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said application program files. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored.

Referring to claim 40, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of determining whether

an originating process that is making said request for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored.

Referring to claim 41, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of a means for examining requests for access to said application program files, a means for determining whether said requests can be granted based on whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a predetermined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy, if said requests are granted then forwarding said requests to a corresponding server that is responsible for serving said application program files. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a means for providing

location information to a local computing system of said application program files that are stored on one or more remote locations.

Referring to claim 42, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of receiving a request from a computer process for access to said application program files, determining if said computer process that is making said request for access is a trusted process, if said computer process is a trusted process, then forwarding said request to a corresponding remote server that is responsible for serving said application program files. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored.

Referring to claims 2, 3, 11, 12, 19, 25, the client application of Safadi would meet the limitation of the dispatch routine that examines the file requests and decides whether to grant or deny said file request (Col. 2, lines 1-10, Col. 3, lines 11-17).

7. Claims 1-3, 10-12, 19, 25, 31-44 are rejected under 35 U.S.C. 102(e) as being anticipated by England, U.S. Patent No. 6,775,779. Referring to claims 1, 10, 19, 25, 31-44, England discloses a system for content protection wherein premium content transmitted from a remote content provider to a client computer is protected from piracy using a hierarchal system of protection (Col. 2, line 66 – Col. 3, line 18 & Col. 4, line 54 – Col. 5, line 34), which meets the

limitation of providing information relating to one or more remote locations where said application program files are stored. The remote content providers can identify trusted modules to run their premium content once received at the client computer (Col. 8, line 64 – Col. 9, line 29). Other modules that are capable of pirating their content are not granted access, which meets the limitation of receiving a request from a computer process for access to said application program files, determining if a history of previous requests for access made by said computer process lacks a pre-determined pattern of piracy, if history of previous requests of said computer process lacks a pre-determined pattern of piracy, then forwarding said request to a corresponding remote server that is responsible for serving said application program files, determining if said computer process that is making said request for access is a trusted process, and forwarding said request to a corresponding remote server if it is a trusted process. With respect to the limitation of accessing a section of said application program files and determining if said section is critical or non-critical, England discusses that the content can be premium or low-value content, and having piracy protection for the premium content and no protection for low-value content because it is simply not worth it (Col. 1, lines 13-38).

Referring to claims 2, 3, 11, 12, the dispatch routine would meet be meet by the security manager in England (Figure 4).

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100